TradingTech Insight | Whitepaper

Getting eComms Surveillance Right

commissioned by NICE · ACTIMIZE

@TradingTechIns

Search TradingTech Insight

www.tradingtechinsight.com

A-Team Insight

NICE · ACTIMIZE

www.niceactimize.com

INTRODUCTION

Emerging innovative technologies like machine learning (ML) and artificial intelligence (AI) are improving the ability of financial services firms to detect and prevent market abuse through the monitoring and analysis of electronic communications (eComms). These technologies are fundamental to new eComms monitoring approaches that solve a range of issues, while reducing risk and keeping compliance costs in check.

In the past, monitoring of eComms (emails, voice, chat, text messages, social media and unified communications) was problematic on many levels, starting with the sheer volume of communications. Retrieving archived eComms related to a specific trade could take weeks. Firms often resorted to employing multiple point solutions for monitoring different communication channels which was costly. Furthermore, bringing multiple channels (for example, telephone, video calling and mobile phones) together to effectively reconstruct a trade was a tedious, time-consuming and highly manual process. Using legacy lexicon-based surveillance approaches might have provided a good front-line of defense, but it also produced large quantities of false positives. This in turn increased the cost of compliance because analysts wasted a lot of time unnecessarily reviewing communications.

Thankfully, over the past few years, eComms surveillance technology has come a long way. Natural language Understanding (NLU), machine learning and other AI techniques enable more precise, intelligent and automated monitoring of all types of communications to help firms more accurately identify risky communications and insider threats, while significantly reducing false positives.

This white paper explores the regulatory outlook on eComms surveillance, the challenges that financial firms are facing with respect to eComms surveillance, and where current technologies fall short. It also offers guidance on how firms can improve the way they monitor eComms by applying new technology to better manage the risks they face.

NICE · ACTIMIZE

www.niceactimize.com

OBSTACLES TO EFFECTIVE ECOMMS SURVEILLANCE

Surveillance of eComms has long proved to be a difficult challenge for financial services firms. Regulations in many jurisdictions require firms to actively monitor communications – and especially those with clients – for potentially criminal activity, including market manipulation and abuse. Effective eComms surveillance, however, has been hampered by the high volumes and different types of communications and data that need to be processed, and the limitations of lexicon-based search technologies that are the basis for most firms' surveillance programs.

Simply put, today's legacy technology is outmatched by the scale and complexity of the challenges. In an attempt to lessen the burden, many firms have resorted to policies that restrict client communications to landlines and emails.

Even with these restrictions in place, firms faced another challenge: how to integrate email and voice communications to form a complete picture of communications with clients. Few firms succeeded in automating this process. When integrated analysis was required, compliance analysts would have to pull the various communications together manually, making financial crimes that straddled these two modes of communication difficult to uncover.

Today these challenges are compounded by many technological factors and regulatory and client expectations:

- **Ineffective search technologies** – While a good, basic first line of defense, primitive lexicon search-based surveillance systems are highly inaccurate. They require compliance analysts to manually maintain a list of words to flag suspicious eComms. This methodology also focuses on finding words rather than understanding the true context of communications and never 'learns' from its mistakes. Some regulating bodies have also found the technology to be sub-standard. FINRA actually fined a large wealth management firm $2 million because the regulator concluded the firm's lexicon-based models were not designed to detect some forms of market abuse.
- **Proliferation of new communication channels** – Thanks to modern technology and consumer preferences, communication channels are growing by leaps and bounds every day. Clients are adopting social media, texting, Skype, mobile phone, and other non-traditional communication methods as their preferred way of conducting business with their financial services firms.

- **Client and regulator expectations regarding eComms** – Instituting an 'only landline calls and emails' eComms policy is no panacea. Firms may think they can squeak by with this approach but it's impractical. Regulators can also easily read between the lines. They know that, inevitably, firms will be pressured by clients to use mobile phones, texting and other communication methods. And they are well aware that employees will resort to these communication methods to avoid detection if they are actively engaging in crimes. The implicit expectation is, that regardless of what the stated policy is, firms should be monitoring these channels.
- **Different detection systems for different channels** – As they evolve their communications policies to allow for more channels, many firms have adopted point solutions to monitor specific forms of eComms. However, these siloed point solutions cannot provide an integrated view of cross-channel conversations between traders and clients. These have to be reconstructed manually, making it is difficult to detect 'intent' and connect the dots.
- **Lack of case management solutions** – Many compliance teams lack even the most basic case management tools to undertake investigations. Instead, they rely on email, spreadsheets, documents and sharing hubs. As a result, analysts often miss important pieces of information or fail to connect the dots. Manual processes are also inadequate for detecting and preventing the types of market abuse that are now happening through a range of electronic methods.

All of the factors above contribute to increased regulatory risk and inefficiencies that drive up costs and increase the risk of fines and reputational damage for financial services firms.

NICE · ACTIMIZE

www.niceactimize.com

ESCALATION OF REGULATORY REQUIREMENTS

Today's regulatory environment around eComms monitoring looks very different from just a decade ago. One catalyst driving the heightened regulations was the London Interbank Offered Rate (LIBOR) scandal, which broke in 2012 after years of allegations in the media. The scandal unearthed widespread activity of false submissions by banks of data about the interest rates they were paying on transactions. It also reawakened concerns about market manipulation in general, and about these activities in non-equity securities trading in particular.

Another catalyst was the 2008 Financial Crisis. The US Dodd-Frank Act, which was enacted shortly thereafter in 2010, significantly strengthened some regulatory requirements around eComms surveillance, including the need to monitor both voice and email activities for potential market abuse, and need to construct trade timelines for regulatory review.

Regulatory authorities have stepped up enforcements and fines too. In 2018, the US Securities and Exchange Commission brought forward 83 actions for either insider trading or market manipulation. In another 2018 example, the Commodity Futures Trading Commission (CTFC) fined a leading brokerage service $50 million after it found that the firm aided and abetted numerous attempts by several of its bank clients to manipulate the ISDAFIX benchmark (a leading global benchmark referenced in a range of interest rate products).

Within the EU, the Market Abuse Regulation (MAR) and the Markets in Financial Instruments Directive (MiFID II) have added new regulatory requirements around market abuse. And the UK's Financial Conduct Authority (FCA) is now focusing on market abuse in a series of Market Watch newsletters, specifically calling out key issues such as firms' failures to calibrate trade surveillance systems and failure to monitor non-equity asset classes in the wake of MiFID II coming into force.

While each jurisdiction has its own specific requirements and enforcement approaches, there are some commonalities. The general regulatory trends in eComms monitoring include the following:

- **Identifying 'intent' now essential** – Today it's no longer enough to simply monitor for actual market abuse events. Firms also need to identify 'intent' to commit market abuse. This intent can be buried deep within a firm's eComms and trade data. While trade data may explain the 'what', communications data can supply the 'why' of financial crimes. Both are essential information for both detection and prosecution.

- **Requiring comprehensive monitoring** – Regulators are no longer satisfied with firms only monitoring a sample of communications. Detecting financial crime is nearly impossible using a sampling approach, and so that methodology is being phased out by regulators. In spite of this, the majority of firms still only examine by batches.
- **Monitoring across channels** – Regulators are keen for firms to extend monitoring beyond 'landline and email' because they know that trading desks are communicating with clients in other ways. Restricting eComms policy to those two channels is now considered antiquated.
- **Outdated or sophisticated** – Regulators are also wary of compliance teams who still rely on outmoded methods, instead of more sophisticated investigation practices. For example, regulators increasingly want compliance teams to be able to create timelines of trades and communications. They also want investigation activities to be auditable.
- **Enforcement on the rise** – Regulators are also cracking down on market abuse. In 2017 alone, the US Financial Industry Regulatory Authority (FINRA) fined 44 firms a total of $8.3 million for eComms violations. Individual fines were as high as $2 million.
- **Deploying SupTech solutions** – Regulators in the US, UK and other jurisdictions are actively engaging in the FinTech revolution, deploying new technology approaches called SupTech. This is making it easier for them to detect market abuse through trade data. The downside is that many of these trade anomalies actually turn out to be cases of market abuse that were undetected by financial services firms themselves due to poor surveillance practices.

Firms that don't keep up with these regulatory demands face a considerable range of growing risks – not just the threat of regulatory sanctions, but also the possibility of unwanted negative headlines and reputational damage. A firm that doesn't police its internal activities properly can be viewed by clients and the broader community as engaging in unethical operations. As a case in point, one of the largest independent broker-dealers was fined $9 million for deficiencies in capturing and monitoring email communications, and this generated wide-spread negative media attention. Getting trade surveillance right is no longer just be a compliance tick-box exercise. It's an imperative that enables firms to deliver on their strategic goals to shareholders.

NICE · ACTIMIZE

www.niceactimize.com

SAILING THROUGH THE PERFECT STORM

Many financial services firms are finding themselves caught in a perfect storm, with increasing regulatory pressures and antiquated technology. Existing, legacy eComms surveillance systems simply cannot deliver the capabilities that firms need to ensure ethical operations and meet tougher regulatory requirements. Exposure to compliance risk and reputational risk is significant, and growing.

But there is a bright side to the storm clouds. Technological advances are radically changing the way eComms surveillance can be conducted today. These advances go a long way toward helping firms reduce their risks and protect their brand, while also improving efficiency and reducing the 'cost of compliance'. These revolutionary technologies include:

- **Cloud computing** – Storing and processing vast quantities of eComms data has become easier through advances in cloud computing. It's now possible to monitor a firm's entire eComms output – millions of data points a day – in lieu of random samples.
- **Big data approaches** – Today's eComms surveillance solutions are breaking down silo barriers to bring together a wide range of communications – from phone calls and emails to social media – and combining that data with trade details to create a comprehensive timeline of all activities around a trade.
- **Metadata techniques** – By analyzing trends in metadata (people, places, things, etc.) today's surveillance technology can also surface unusual behaviors that employees and clients are engaging in, an early signal of risky activities.
- **Machine learning** – Supervised and unsupervised machine learning techniques have also been proven to substantially reduce false positive rates. Machine learning can be applied to alert generation, parameter setting, system calibration, risk scoring, and segmentation.
- **Natural language understanding** – This form of machine learning has evolved considerably, enabling better detection results from text documents and transcribed voice recordings too. NPU is now being applied to a wide range of languages, too, both in written and in oral form to comprehend the true context of conversations and more accurately flag risky communications.
- **Artificial intelligence** – Today's technology, which combines artificial intelligence-based modelling with sophisticated workflows, also reduces false positives, makes case management more efficient, and enables firms to understand what their data is 'telling' them in new, insightful ways.

The applications of these new technologies to the perplexing challenges of eComms surveillance is very promising, but financial services organizations should never accept solutions at face value. They should diligently investigate all options to ensure their chosen solution will deliver lower false positives, is easy to use, and will accurately detect inappropriate behavior. Above all, in today's world of FinTech and RegTech hype, it's important to partner with a company that can deliver on its promises and has a solid reputation.

NICE · ACTIMIZE

www.niceactimize.com

THE SOLUTION

Purchasing a new eComms surveillance solution can seem daunting – it's important to work with a company whose solution can deliver on the promises of recent technological advances.

INTELLIGENT ECOMMS SURVEILLANCE

For firms relying on outdated, legacy technology, there has never been a better time to upgrade surveillance capabilities. With an intelligent eComms surveillance solution built for today's complex regulatory and multi-channel environment, firms can better manage regulatory risk, protect their brand, vastly improve compliance analyst productivity, and keep compliance costs in check.

The NICE Actimize Intelligent eComms Surveillance solution – created by a technology company that financial services firms can trust – empowers compliance teams to analyze communications and trades quickly to root out problematic transactions. Specifically, it's able to:

- **Analyze 100% of a Trader's Conversations** – NICE Actimize's Intelligent eComms Surveillance solution tracks conversations across a wide range of channels. It is also able to combine all communications with trade data for a complete timeline, to help analysts uncover hidden conduct risks, collusion, and insider trading. It supports hundreds of data types, which means it can connect to, ingest and index data from storage vaults containing emails, chats, text messages, social media, and even voice. The solution's transcription engine, powered by NICE Nexidia, can understand audio in 44 different languages.
- **Reduce False Positives by >50%** – Powered by artificial intelligence and automation, NICE Actimize's Intelligent eComms Surveillance solution uses Natural Language Understanding (text analytics and linguistics), smart classification and advanced speech and behavioral analytics (all fine-tuned for financial markets). This enables the solution to comprehend the true context of conversations and accurately flag risks in communications across all communication channels. Nice Actimize's intelligent analytics automatically detects people, places, products, companies, trades, asset classes, and conversation topics within eComms and transcribed voice conversations. It is able to understand the context of conversations and provide unique insight into

what regulated employees actually said and did. Additionally, both supervised and unsupervised machine learning enables the analytics to get even smarter over time, further improving detection accuracy.

- **Boosts Compliance Analyst Productivity** – NICE Actimize's award-winning, AI-enabled ActOne integrated crime investigation management solution works hand-in-hand with other rich capabilities of the eComms solution to cut investigation time from hours to minutes. ActOne features built-in workflows that automate and accelerate the entire investigation process. Each time compliance analysts log on, they're presented with a queue of flagged conversations to review, and policy-driven workflows guide them through each stage of the investigation. Analysts can instantly escalate a case and even launch an automated trade reconstruction tool to reconstruct complete communications and trade timelines with the click of a mouse.

For more information on how Nice Actimize can help, visit www.niceactimize.com/compliance and @NICECompliance, or contact NICE Actimize at compliance@niceactimize.com.

NICE · ACTIMIZE

www.niceactimize.com

ABOUT NICE ACTIMIZE

NICE Actimize (Nasdaq: NICE) is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

NICE · ACTIMIZE

ABOUT A-TEAM GROUP

A-Team Group helps financial technology vendors and consultants – large and small – to grow their businesses with content marketing. We leverage our deep industry knowledge, ability to generate high quality media across digital, print and live platforms, and our industry-leading database of contacts to deliver results for our clients. For more information visit **www.a-teamgroup.com**

A-Team Group's content platform is A-Team Insight, encompassing our RegTech Insight, Data Management Insight and TradingTech Insight channels.

A-Team Insight is your single destination for in-depth knowledge and resources across all aspects of regulation, enterprise data management and trading technology in financial markets. It brings together our expertise across our well-established brands, it includes:

RegTech Insight focuses on how data, technology and processes at financial institutions are impacted by regulations. **www.regtechinsight.com**

Data Management Insight delivers insight into how financial institutions are working to best manage data quality across the enterprise. **www.datamanagementinsight.com**

TradingTech Insight keeps you up to speed with the dynamic world of front office trading technology and market data. **www.tradingtechinsight.com**

You can tailor your experience by filtering our content based on the topics you are specifically interested in, across our range of blogs with expert opinions from our editors, in-depth white papers, supplements and handbooks, and interactive webinars, and you can join us in person at our range of A-Team Summits and briefings. Visit **www.a-teaminsight.com**

Become an A-Team Insight member – it's free!
Visit: **www.a-teaminsight.com/membership**.